Functional req

Monday, March 21, 2022 5:01 PM

for the merchant

- 1 sign up
  - Sign up with email and user name and password and confirmPassword
    - Password must be at least 10 charters and strong
  - Account must be activated by sending a message to the given email that has a OTP (on time password) that must be provided within 10 minutes or it will be valid
  - You must save the date that this account has been made in and mark it activated or not
  - Account will be in test mode when it is first created
- 2 log in
  - Your must log in with the right email and password
    He will be given 6 tries for the password for the same email if wrong he will be stopped for an hour
  - If 2 way Auth is enabled he will have to provide the OTP to login
  - He will get the access and refresh token when logging in successfully
  - His IP and device info and refresh token will be saved -----------
- 3 signing out
  - Will signing out the refresh token will be deleted
- 4 forgetting password
  - A rest link will be sent to the email if valid
  - The rest link will has a token that only valid to 10 m
  - It a wrong token provided or expired one the new password will be rejected
  - Will add his new password in this link
- 5 editing his profile
  - Can change his name
  - Can change is password by providing the old one and the new
- 6 clear login sessions
  - Can see every session that he has logged in from
  - Can see the device and the IP address and the time
  - Can sign out from them
- 7 can disable is account

- For the admin
  - 1Log in with account that has been made manually in the database for an admin as a role
  - 2 see all info about all available merchants accounts
    - can only see 20 merchant per page
    - Can filter by email
    - Can filter by activated for not
    - Can filter by active or not
  - 3 can disable or inactivate any account and delete any account

Non-functional req

Monday, March 21, 2022 5:01 PM

- Security
  - Will use JWT token for authentication
    - Wil apply refresh token for more security
    - The access token will valid for 30 min and
    - The refresh token can be valid for only 1 week
  - Set all the security standers headers to the request
  - CORS
  - Rate Limiting
    - The user can only send some number for req in certain time -- will see what is the best number for this still
  - Limit the body size for the req to 20kb -- still can change that
  - Sanitizing data
    - Against noSQL injection
    - XSS
    - Parameter pollution
  - Maximum login attempts
  - Prevent regulars expressions
  - System cant send any error details in production
  - Prevent CSURF
  - Two-factor authentication must be enabled for activated users